FPKIMA Newsletter

Winter 2016
Volume 3 Issue 1

Federal PKI Management Authority
Enabling Trust

Inside This Issue

The National Institute of Standards and Technology (NIST) hosted a two-day Advanced Identity Workshop on January 12 and 13th. The intent of the workshop was to brainstorm how to create a stronger, measurement-based approach to evaluating the strength of a digital identity and give consumers and service providers a better way to make sound, risk-based access decisions. A summary of the workshop will be available in March 2016 with a further period for comment. Workshop reference white papers are also available at http://www.nist.gov/nstic/whitepapers.html

Biometric Authentication and Beyond

If 2015 was the year of the breach, 2016 will be the year of stronger authentication. The use of other-than-password authentication has significantly grown in the past year with increased adoption forecasted in 2016. From password killers to biometrics, companies and the government are taking on the challenge to eradicate password usage or at a minimum require passwords be combined with another form of authentication, referred to as two-factor authentication. NIST has recommended since 2009 to only use passwords in low-risk systems and if passwords are needed, they should be supplemented with stronger forms of authentication such as biometrics, one-time passwords, or PIV cards.

Password Killers

NIST, Yahoo, and Google are just of a few of the driving forces behind finding new "password killing" authentication methods. NIST is the point agency to develop an "identity ecosystem" that fulfills the vision of the National Strategy for Trusted Identities in Cyberspace (NSTIC). The intent of the ecosystem is to allow any user to use multiple forms of authentication to access industry or government assets instead of creating a new password. Yahoo has almost removed the use of the password by implementing a trusted device service where access to Yahoo mail can only be granted if approved from a pre-registered device. The company Alphabet, formerly Google, is currently testing the use of a smart device as a biometric sensor for authentication. Part of a program called "Project Abacus;" the desired result is that a user could unlock or lock devices and apps based on a "trust score" calculated on his or her smart device using location patterns, voice and speech patterns, facial recognition, and how the user walks and types. While none of these are perfect solutions, there is great potential to provide more convenient and secure authentication methods than a password.

Biometrics

Apple Touch ID, a fingerprint recognition feature, and Samsung fingerprint scanner have brought easy and secure biometric authentication to the masses; they are integrated into not only device access, but application and payment systems. Banks have started implementing iris scanning ATMs to reduce ATM transaction fraud. Microsoft also unveiled a new Lumia phone that integrates with the Windows 10 biometric security system to allow users access to iris recognition authentication capabilities. FIPS 201-2 also outlines a standard for capturing biometrics for use with PIV card authentication. PIV and PIV-I cards following either FIPS 201-2 or the FPKI Federal Bridge Certificate Policy for PIV-I have the capability for either fingerprint or iris authentication, both of which provide a stronger form of multifactor authentication.

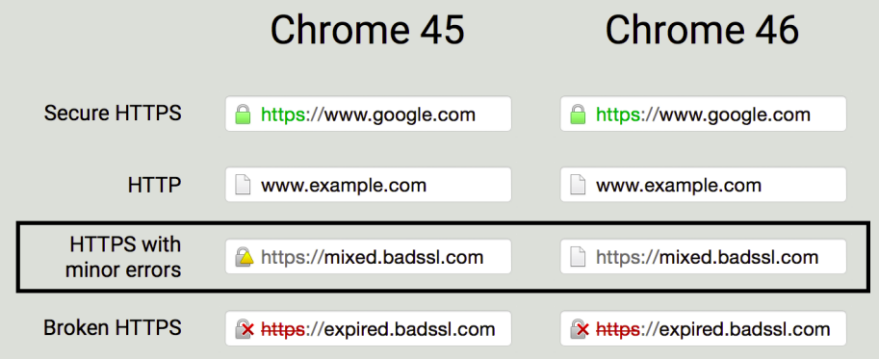
Based on authentication trends for 2016, the use of more secure and user friendly authentication is dependent on mobile or smart device integration. Is your agency using biometrics or mobile devices for remote or application authentication? Let us know and be featured in a future newsletter: FPKIPA-MA@listserv.gsa.gov.

SSL SHA1 Deprecation and HTTPS Update

Browsers have implemented increased web security

Over the past several years, security has become increasingly important in securing web-based transactions. HTTP Secure (HTTPS) which is security through the use of a TLS/SSL PKI certificate is becoming the default configuration and is required by many browsers. The major browser vendors (Microsoft, Apple, Google, and Mozilla) have recently implemented improved website security practices through the use of security indicators and warning pages.

Google, as an incentive to move to HTTPS, has increased the search ranking for pages with HTTPS and is driving the status quo of making HTTPS the default. Google believes that the best way to guarantee that a web site is authentic is when it uses HTTPS with no errors. This is the driving logic behind Google implementing new security icons in the latest and future versions of Chrome. Google is even contemplating flagging HTTP pages with a red "x" because the website owner is not using any security to ensure its users are on an authentic website.



Example of Google Chrome Website Security Icons

Mozilla Firefox is the other leading adopter of improved web site security warnings and has taken a similar position on HTTPS as the only true measure of website authentication. Both Mozilla and Google handle errors and mixed content in a similar fashion. Mixed content is where videos or pictures on a website may originate from a non-secure source and potentially intercept a transaction thought to be secured. Even though each browser may handle errors differently, there is a common agreement among browsers to indicate websites are secure by displaying a lock or organization name in the color green. Anything in the address bar besides the color green means there is an issue with either the content on the site or with the SSL certificate. If a user encounters anything besides a green lock or bar, they should report the issue to the website owner so it can be corrected.

Example of Mozilla Firefox Website Security Icons

PIV-I Change Proposal Approved!

The Federal PKI Policy Authority approved a change proposal to align PIV-I with FIPS 201-2 and extend PIV-I card life from five to six years. It also added the requirement for annual card testing similar to PIV. Please send any questions to fpki-compliance@gsa.gov

Explore the Government Acquisition Gateway yet?

The Acquisition Gateway, otherwise known as the Common Acquisition Platform (CAP) and built by GSA, helps federal government buyers from all agencies act as one acquisition community. The Acquisition Gateway features information on government-wide contract vehicle comparisons, acquisition best practices, market research tools, prices paid data, and other useful tools and features. The website is open to federal and non-federal users with full site access for federal acquisition employees and approved contractors. Sign up at https://hallways.cap.gsa.gov/

Did you know…?

The Federal Identity, Credential, and Access Management (FICAM) Architecture and Playbook Tiger Team (APTT) has released a new draft of the FICAM Segment Architecture! Following DigitalGov's guide of open collaboration, the FICAM APTT released the draft document, known as the FICAM Roadmap and Implementation Guidance, on GSA's GitHub website for all government and citizen users to contribute and comment on content.

The intent is for progressive updates as technology changes to build a long-term and collaborative replacement to the current document. The posted interactive guide provides a conceptual diagram, goals and objectives, service framework, use cases, and much more. Some sections still need content so provide your input at https://gsa.github.io/ficam-arch/

NSTIC Pilot Programs

Federal Pilots Lower Identity Ecosystem Barriers

NSTIC outlines four guiding principles to creating an Identity Ecosystem which are technologies that enhance privacy and are secure, interoperable, and cost-effective. To help lower the barriers to realizing the guiding principles of NSTIC, NIST annually funds pilot projects to increase adoption of innovative authentication techniques, privacy-enhancing technologies, and other potential cost effective and secure options to building and using trusted identities. The complete list of pilots can be found on http://www.nist.gov/nstic/pilots.html with a few of them listed below.

- **Georgia Tech Research Corporation (GTRI)** (2013) was selected to develop and demonstrate a Trustmark Framework. A Trustmark is a badge, image, or symbol to indicate that a website business is shown to be trustworthy. Defining trustmarks and trust framework providers to internet users will improve the trust and privacy of using the Identity Ecosystem.
- **HealthIDx** (2015) is developing a "triple-blind" privacy-enhancing technology to protect patients' identity and information. A medical service provider has no knowledge of which credential service provider an end-user chooses, credential service providers have no knowledge of which medical service provider the end-user is visiting, and the identity broker has no knowledge or ability to retain information about the transaction's parties or contents.
- **ID.me** (2013) has focused on expanding the number and use of NSTIC-aligned credentials by developing identity solutions that give military, veterans, first responders, and students access to discounts at hundreds of companies. They've also worked to educate the public and companies on the benefits of accepting NSTIC-aligned credentials. ID.me has issued over a million credentials and is approved as a credential service provider by GSA's Trust Framework Solutions program.
- **MorphoTrust** (2014 – 2015) has two pilots focusing on preventing theft of personal state tax refunds by creating interoperable and trustworthy electronic IDs that individuals control. The 2nd pilot is a partnership with the State of North Carolina to extend a state-issued driver's license into a digital credential to reduce identity provisioning costs and increase state residents access to benefits.
- **Resilient Network Systems** (2012) demonstrated the secure exchange of sensitive health and education transactions. Resilient's Trust Network was built around privacy-enhancing encryption technology to provide secure, multifactor, on-demand identity proofing and authentication.
- **GSMA** (2014) has partnered with AT&T, Sprint, T-Mobile, and Verizon to create an NSTIC-aligned mobile-based credential to allow relying parties to more easily accept identity solutions from any partner network.
- **Confyrm** (2014) will demonstrate methods to minimize risk in accepting federated identities. One major risk of accepting federated credentials is the possibility it could be compromised or faked. Confyrm developed a model to signal account takeovers and fake accounts through fraud detection and notification.

Annual PIV / PIV-I Card Testing

NIST updated the special publication 800-79 in July 2015 following the update to FIPS 201-2 and the introduction of Derived Credentials. The intent of NIST 800-79-2 is to outline requirements and create an assessment framework for PIV Card Issuers and Derived PIV Credential Issuers (PCI and DPCI) to follow to ensure credentials are issued according to the policy. NIST 800-79 also outlines an annual assessment to ensure continued compliance. The GSA FIPS 201 Evaluation Program office supports annual assessments by conducting annual PIV testing to promote and ensure PIV interoperability and identify potential disconnects and misconfigurations of credentials.

As part of this annual assessment, a PCI/DPCI should submit a PIV card to the GSA FIPS 201 Evaluation Program for testing with the 85B tool which is a PIV test program designed after the PIV data model test guidelines in NIST SP 800-85B. Agencies and issuers are encouraged to obtain a copy of the 85B tool from the FIPS 201 office prior to having an 800-79 assessment to help identify possible issues that may arise.

PIV-I issuers are not required to have an 800-79 assessment, but are required to submit a PIV-I card for annual testing per the latest approved change proposal. PIV-I card issuers are also encouraged to obtain a copy of the 85B tool and submit test results prior to official testing. Because PIV and PIV-I card testing also requires biometrics, a production card should be issued and used for testing.

For more information about annual PIV and PIV-I testing, send an email to fpki-compliance@gsa.gov.

Ask the FPKIMA

What kind of questions and issues should I send to the FPKI help desk?

The FPKI help desk is meant to help with issues related to validation and availability of the FPKIMA certification authorities (CAs) which include the Federal Common Policy CA, the Federal Bridge CA, SHA1 Federal Root CA, and the eGovernance Trust Services CA. Some examples of typical help desk questions include requesting a secure distribution of one of the FPKIMA CAs, trouble in validating a certificate to one of the FPKIMA CAs, or general questions about the FPKIMA.

The FPKI help desk may not be able to help with PKI enabling questions or resolving issues that do not have a root cause from one of the FPKIMA CAs, but could be a good starting point to find the correct party.

Where Can I Find More Information on the FPKIMA?

FPKIMA information can be found on the idmanagement.gov website:
https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XNNc

Federal PKI Management Authority
Enabling Trust

Need Help?

Contact the FPKIMA

fpki-help@gsa.gov

The NIST National Cybersecurity Center of Excellence (NCCOE) released a draft Cybersecurity practice guide on Attribute Based Access Control (ABAC) with a how-to guide using a standards-based approach of current technology and software. ABAC is an advanced method for automating access rights for people and systems connecting to network and assets based on a user's attributes, such as an IP address, certifications, employee status, location, job, etc. Most agencies and businesses use Role-Based Access Control (RBAC) to assign access based on static values of job title or a defined role that require manual changes across multiple systems and applications.

Learn more at https://nccoe.nist.gov/projects/building_blocks/attribute_based_access_control